## Ch5: Review Questions

**5-1 What are the components of IT infrastructure?**

Define information technology (IT) infrastructure and describe each of its components.

A firm’s IT infrastructure provides the foundation, or platform, for supporting all the information systems in the business.

The five major components of an information technology (IT) infrastructure are:

* **Computer hardware:** technology for computer processing, data storage, input, and output.
* **Computer software:** includes both system software and application software.
* **Data management technology:** organizes, manages, and processes business data concerned with inventory, customers, and vendors.
* **Networking and telecommunications technologies:** provide data, voice, and video connectivity to employees, customers, and suppliers.
* **Technology services:** external consultants who run and manage infrastructure components.

5-2 What are the major computer hardware, data storage, input, and output technologies used in business and major hardware trends?

List and describe the various types of computers available to businesses today.

* **Personal computers:** Generally used when working alone or with a few other people in a small business.
* **Workstations:** Desktop computers with more powerful mathematical and graphics-processing capabilities than a PC. Used primarily for advanced design or engineering work requiring powerful graphics or computational capabilities.
* **Servers:** Specifically optimized to support a computer network, enabling users to share files, software, peripheral devices, or other network resources.
* **Mainframes:** Large-capacity, high performance computers that process vast amounts of data very rapidly.
* **Supercomputers:** Specially designed and more sophisticated computers used for tasks requiring extremely rapid and complex calculations with thousands of variables, millions of measurements, and thousands of equations.
* **Grid computing:** Geographically remote computers connected into a single network to create a “virtual supercomputer” by combining the computational power of all computers on the grid.

Define the client/server model of computing and describe the difference between a two-tiered and N-tier client/server architecture.

Client/server computing splits processing between “clients” and “servers.” Both are on the network but each machine is assigned functions it is best suited to perform. The client is the user point of entry for the required function and is normally a desktop computer, workstation, or laptop computer. The user generally interacts directly only with the client portion of the application, often to input data or retrieve data for further analysis. The server provides the client with services. Servers store and process shared data and also perform back-end functions not visible to users, such as managing network activities.

Two-tiered client/server architecture is the simplest form of client/server network. It consists of a client computer networked to a server computer, with processing split between the two types of machines.

N-tier client/server architecture is more complex than the simple two-tiered client/server network. In this type of architecture, the work of the entire network is balanced over several different levels of servers, depending on the kind of service being requested.

Define and describe the mobile digital platform, BYOD, nanotechnology, grid computing, cloud computing, virtualization, green computing, and multicore processing.

**Mobile digital platform:** More and more business computing is moving from PCs and desktop machines to mobile devices like cell phones and smartphones. Data transmissions, web surfing, email and instant messaging, digital content displays, and data exchanges with internal corporate systems are all available through a mobile digital platform. Netbooks, small low-cost lightweight subnotebooks that are optimized for wireless communication and internet access, are included.

**BYOD: B**ring **Y**our **O**wn **D**evice: Is a concept in which companies allow employees to use personal computing devices to access corporate networks. Devices may include cell phones, tablet computers, or other handheld computing devices. It’s one aspect of the ‘consumerization of IT’ in which new information technology that first emerges in the consumer market spreads into business organizations.

**Nanotechnology:** Uses individual atoms and molecules to create computer chips and other devices that are thousands of times smaller than current technologies permit. Nanotechnology shrinks the size of transistors down to the width of several atoms.

**Grid computing:** Connects geographically remote computers into a single network to create a “virtual supercomputer” by combining the computational power of all computers on the grid.

**Cloud computing:** A model of computing where firms and individuals obtain computing power and software applications over the internet, rather than purchasing their own hardware and software. Data are stored on powerful servers in massive data centers, and can be accessed by anyone with an internet connection and standard web browser. Cloud computing consists of three types of services:

* *Cloud infrastructure as a service:* customers use processing, storage, networking, and other computing resources from cloud service providers to run their information systems.
* *Cloud platform as a service:* customers use infrastructure and programming tools hosted by the service provider to develop their own applications.
* *Cloud software as a service:* customers use software hosted by the vendor.

**Virtualization:** Is the process of presenting a set of computing resources (such as computing power or data storage) so that they can all be accessed in ways that are not restricted by physical configuration or geographic location. Server virtualization enables companies to run more than one operating system at the same time on a single machine.

**Green computing:** Refers to the practices and technologies for designing, manufacturing, using and disposing of computers, servers, and associated devices such as monitors, printers, storage devices, and networking and communications systems to minimize their impact on the environment. Reducing computer power consumption has been a very high “green” priority because technology is responsible for about two percent of the total U.S. power demand.

**Multicore processing:** Uses integrated circuits to which two or more processors have been attached for enhanced performance, reduced power consumption, and more efficient simultaneous processing of multiple tasks.

**5-3 What are the major types of computer software used in business and major software trends?**

Distinguish between application software and system software and explain the role played by the operating system of a computer.

System software surrounds and controls access to the hardware. It manages and controls a computer’s activities. Some types of system software consist of computer language translation programs that convert programming languages into machine language that can be understood by the computer and utility programs that perform common processing tasks, such as copying, sorting, or computing a square root. The operating system allocates and assigns system resources, schedules the use of computer resources and computer jobs, and monitors computer system activities.

Application software works through the system software in order to develop specific business applications. This type of software includes traditional programming languages, fourth-generation languages, application software packages and desktop productivity tools, software for developing internet applications, and software for enterprise integration.

List and describe the major PC and server operating systems.

Table 5.3 describes the leading PC and server operating systems.

* **Windows 10:** Most recent Windows operating system.
* **Windows Server:** Most recent Windows OS for servers.
* **UNIX:** Used for powerful PCs, workstations, and network servers. Supports multitasking, multi-user processing, and networking. It is portable to different models of computer hardware.
* **Linux:** Open source, reliable alternative to UNIX and Windows OS that runs on many different types of computer hardware. Can be modified by software developers.
* **OS X and macOS:** OS for Macintosh computers that is stable and reliable, with powerful search capabilities, support for video and image processing, and an elegant user interface. Most recent version is macOS Sierra. The iPhone operating system is derived from OS X.

Name and describe the major desktop productivity software tools.

**Word processing:** Allows users to make changes in the document electronically in memory, eliminating the need to retype entire pages to make corrections. It often includes advanced features such as spelling checkers and thesaurus programs.

**Spreadsheets:** Composed of a grid of columns and rows, spreadsheets are good at performing calculations on interrelated pieces of data. Used for applications in which numerous calculations with pieces of data must be related to each other. When you change a value or values, all other related values on the spreadsheet will be automatically recomputed. Spreadsheets provide computerized versions of traditional financial modeling tools and provide an easy-to-use method of performing what-if analysis.

**Data management:** Used for creating and manipulating lists and for combining information from different fields. Data management software typically has facilities for creating files and databases to store, modify, and manipulate data for reports and queries.

**Presentation graphics:** Allow users to create professional quality graphics presentations. This software can convert numeric data into charts and other types of graphics and can include multimedia displays of sound, animation, photos, and video clips.

**Software suites:** Combine the functions of the most important microcomputer software packages, such as spreadsheets, word processing, graphics, and data management. This integration provides a more general-purpose software tool and eliminates redundant data entry and data maintenance. Some low-cost desktop productivity suites can be downloaded from the web.

**Web browsers:** Easy-to-use software tools for accessing the web and the internet. Web browsers have become the primary interface for accessing the internet or for using networked systems based on internet technology.

Explain how Java and HTML are used in building applications for the web.

**Java** is used for building applications that run on the web and HTML is used for creating webpages. Java is an operating system that is processor-independent. Its object-oriented programming language has become the leading interactive programming environment for the web. Java enables users to manipulate data on networked systems using web browsers, reducing the need to write specialized software.

**Hypertext markup language (HTML)** is a page description language for specifying how text, graphics, video, and sound are placed on a webpage and for creating dynamic links to other webpages and objects. HTML programs can be custom written, but they also can be created using the HTML authoring capabilities of web browsers or of popular word processing, spreadsheet, data management, and presentation graphics software packages. HTML editors are more powerful HTML authoring tool programs for creating webpages.

Define web services, describe the technologies they use, and explain how web services benefit businesses.

Web services are sets of loosely coupled software components that exchange information with each other using universal web communications standards and languages. They can be used as components of web-based applications linking the systems of two different organizations or to link disparate systems of a single company. Web services are not tied to a particular operating system or programming language. Different applications can use them to communicate with each other in a standard way without time-consuming custom coding.

XML is the foundation technology for web services. This language makes it possible for computers to manipulate and interpret their data automatically and perform operations on the data without human intervention.

Businesses use web services to tie their websites with external websites, creating an apparently seamless experience for users. The benefit derives from not having to re-create applications for each business partner or specific function within a single company.

Explain why open-source software is so important today and its benefits for business.

Open-source software is not owned by any company or individual. A global network of programmers and users manage and modify the software, fix errors in it, or make improvements to its functionality. By definition, open-source software is not restricted to any specific operating system or hardware technology. Several large software companies are converting some of their commercial programs to open source.

Linux is the most well-known open-source software. It’s a UNIX-like operating system that can be downloaded from the internet, free of charge, or purchased for a small fee from companies that provide additional tools for the software. It is reliable, compactly designed, and capable of running on many different hardware platforms, including servers, handheld computers, and consumer electronics. Linux has become popular during the past few years as a robust low-cost alternative to UNIX and the Windows operating system.

Thousands of open-source programs are available from hundreds of websites. Businesses can choose from a range of open-source software including operating systems, office suites, web browsers, and games. Open-source software allows businesses to reduce the total cost of ownership. It provides more robust software that’s often more secure than proprietary software.

List and describe cloud computing software services, mashups, and apps and explain how they benefit individuals and businesses.

**Cloud computing** is becoming popular for describing web-based applications that are stored and accessed via the “cloud” of the internet. The software and the data they use are hosted on powerful servers in massive data centers, and can be accessed by anyone with an internet connection and standard web browser. The best examples are Google Apps desktop productivity tools and Microsoft’s Live software suite.

**Mashups** are new software applications and services based on combining different online software applications using high-speed data networks, universal communication standards, and open-source code. Users are able to create new software applications and services based on combining different online software applications. These new combined applications depend on high-speed data networks, universal communication standards, and open-source code. The idea is to take different sources and produce a new work that is “greater than the sum” of its parts. Web mashups combine the capabilities of two or more online applications to create a kind of hybrid that provides more customer value than the original sources alone.

**Apps** are small pieces of software that run on the internet, on a computer, or on a mobile phone or tablet to provide additional functionality. Most of the attention goes to the apps that have been developed for the mobile digital platform. Apps turn smartphones and other mobile handheld devices into general-purpose computing tools.

Businesses benefit most from these new tools and trends by not having to re-invent the wheel. Apps have already been developed by someone else and a business can use them for its own purposes. Mashups let a business combine previously developed web applications into new ones with new purposes. They don’t have to re-invent the previous applications from scratch—merely use them in the new processes. Organizations using cloud computing generally do not own the infrastructure. Instead, they purchase their computing services from remote providers and pay only for the amount of computing power they actually use.

**5-4 What are the principal issues in managing hardware and software technology?**

Explain why managers need to pay attention to capacity planning and scalability of technology resources.

The principle issues in managing hardware and software assets include capacity planning and scalability. Capacity planning is the process of predicting when a computer hardware system becomes saturated. It considers factors such as the maximum number of users that the system can accommodate at one time; the impact of existing and future software applications; and performance measures, such as minimum response time for processing business transactions. Capacity planning ensures that the firm has enough computing power for its current and future needs.

Scalability refers to the ability of a computer, product, or system to expand to serve a large number of users without breaking down. Organizations must ensure they have sufficient computer processing, storage, and network resources to handle surging volumes of digital transactions and to make such data immediately available online.

Describe the cost components used to calculate the total cost of ownership (TCO) of technology assets.

When calculating the total cost of ownership of technology assets, a business must include the original cost of the hardware and software, installation costs, ongoing administration costs for hardware and software upgrades, maintenance, technical support, training, downtime, and even utility and real estate costs for running and housing the technology.

“Hidden costs” for support staff, downtime, and additional network management can make distributed client/server architectures—especially those incorporating handheld computers and wireless devices—more expensive than centralized mainframe architectures.

Identify the benefits and challenges of using outsourcing, cloud computing services, and mobile platforms.

In the past, most companies ran their own computer facilities and developed their own software. Today, more and more companies are obtaining their hardware and software technology from external service vendors.

**Outsourcing:** The most important benefit of outsourcing technology management is that it allows a business to concentrate on its core competencies rather than focusing on technology issues. Instead of purchasing all the necessary hardware and software for hosting a website, a business can use a web hosting service that maintains a large web server, or a series of servers, and provides fee-paying subscribers with space to maintain their websites.

Outsourcing custom software development or maintenance to outside firms benefits a company because it won’t have to hire programmers, analysts, and managers with the necessary skills. An outsourcer often has the technical and management skills to do the job better, faster, and more efficiently. Even though it’s often cheaper to outsource the maintenance of an IT infrastructure and the development of new systems to external vendors, a business must weigh the pros and cons carefully. Service level agreements are formal contracts between customers and service providers that define the specific responsibilities of the service provider and the level of service expected by the customer.

**Cloud computing services:** Refer to services that deliver and provide access to hardware and software remotely as a web-based service. A business can rent software from another firm and avoid the expense and difficulty of installing, operating, and maintaining the hardware and software on its own. A business must carefully assess the costs and benefits of the service, weighing all people, organizational, and technology issues. It must ensure it can integrate the software with its existing systems and deliver a level of service and performance that is acceptable for the business.

Small and medium-sized businesses may find it more advantageous to use cloud computing services because of the minimal overhead and upfront costs. Large businesses will have to factor in whether cloud computing capabilities are sufficiently secure or reliable for their most critical systems. These firms may choose to handle their average processing loads in-house and pay for only as much additional computing power as the market demands. This arrangement enables firms to have a more flexible infrastructure, some of it owned by the firm, and some of it rented from giant computer centers run by technology specialists.

**Mobile platforms:** Integrating mobile platforms with the firm’s existing IT infrastructure and applications may be quite a challenge for many organizations. Central coordination and oversight are essential. Firms must inventory the mobile devices and develop policies and tools for tracking, updating, and securing them and for controlling the data and applications that run on them. Gains in employees’ productivity and efficiency must be balanced against increased costs of integrating the devices into the firm’s IT infrastructure and from providing technical support. The total cost of ownership for each device is much higher than typical IT hardware.

**Explain why software localization has become an important management issue for global companies.**

A global organization must create systems that can be realistically used by multiple business units in different countries. Software applications may require local language interfaces including menu bars, commands, error messages, reports, queries, online data entry forms, and system documentation. The interfaces must be easily understood and mastered quickly in a variety of languages. Global systems must also consider differences in local cultures and business processes.

**Ch 6: Review Questions**

6-1 What is a database and how does a relational database organize data?

Define a database.

A group of related files makes up a database. Databases are at the heart of all information systems because they keep track of the people, places, and things that a business must deal with on a continuing, often instant basis.

Define and explain the significance of entities, attributes, and key fields.

* *Entity* is a person, place, thing, or event on which information can be obtained.
* *Attribute* is a piece of information describing a particular entity.
* *Key field* is a field in a record that uniquely identifies instances of that record so that it can be retrieved, updated, or sorted. For example, a person’s name cannot be a key field because there can be another person with the same name, whereas a social security number is unique. Also, a product name may not be unique but a product number can be designed to be unique.

Define a relational database and explain how it organizes and stores information.

The relational database is the primary method for organizing and maintaining data in most modern information systems. It organizes data in two-dimensional tables with rows and columns called relations. Each table contains data about an entity and its attributes. Each row represents a record and each column represents an attribute or field. Each table also contains a key field to uniquely identify each record for retrieval or manipulation.

(Learning Objective 1: What is a database and how does a relational database organize data?, AACSB: Application of knowledge.)

Explain the role of entity-relationship diagrams and normalization in database design.

Relational databases organize data into two-dimensional tables (relations) with columns and rows. Each table contains data on an entity and its attributes. An entity-relationship diagram graphically depicts the relationship between entities (tables) in a relational database. A well-designed relational database will not have many-to-many relationships, and all attributes for a specific entity will only apply to that entity.

Normalization is the process of creating small stable data structures from complex groups of data when designing a relational database. Normalization streamlines relational database design by removing redundant data, such as repeating data groups. A well-designed relational database will be organized around the information needs of the business and will probably be in some normalized form. A database that is not normalized will have problems with insertion, deletion, and modification.

**6-2 What are the principles of a database management system?**

**Define a database management system (DBMS), describe how it works, and explain how it benefits organizations.**

A database management system (DBMS) is a specific type of software for creating, storing, organizing, and accessing data from a database. A DBMS consists of software that permits centralization of data and data management so that businesses have a single, consistent source for all their data needs. A single database services multiple applications. The most important feature of the DBMS is its ability to separate the logical and physical views of data. The user works with a logical view of data. The DBMS retrieves information so that the user does not have to be concerned with its physical location.

**Define and compare the logical and physical views of data.**

The DBMS relieves the end user or programmer from the task of understanding where and how the data are actually stored by separating the logical and physical views of the data. The logical view presents data as end users or business specialists would perceive them, whereas the physical view shows how data are actually organized and structured on physical storage media, such as a hard disk.

**Define and describe the three operations of a relational database management system.**

In a relational database, three basic operations are used to develop useful sets of data: select, project, and join.

* **Select operation:** Creates a subset consisting of all records in the file that meet stated criteria. In other words, select creates a subset of rows that meet certain criteria.
* **Join operation:** Combines relational tables to provide the user with more information than is available in individual tables.
* **Project operation:** Creates a subset consisting of columns in a table, permitting the user to create new tables that contain only the information required.

**Name and describe the three major capabilities of a DBMS.**

A DBMS includes capabilities and tools for organizing, managing, and accessing the data in the database. The principal capabilities of a DBMS include a data definition language, data dictionary, and data manipulation language.

* The data definition language specifies the structure and content of the database.
* The data dictionary is an automated or manual file that stores information about the data in the database, including names, definitions, formats, and descriptions of data elements.
* The data manipulation language, such as SQL, is a specialized language for accessing and manipulating the data in the database.

**Define non-relational databases and describe their capabilities.**

Non-relational database management systems use a more flexible data model and are designed for managing large data sets across many distributed machines and for easily scaling up or down.

There are four main reasons for the rise in non-relational databases: cloud computing, unprecedented data volumes, massive workloads for web services, and the need to store new types of data.

Non-relationship databases can process structured and unstructured data captured from websites, social media, and graphics. Traditional relational databases aren’t able to process data from most of those sources. Non-relational databases can also accelerate simple queries against large volumes of structured and unstructured data. There’s no need to pre-define a formal database structure or change that definition if new data are added later.

**6-3 What are the principal tools and technologies for accessing information from databases to improve business performance and decision making?**

Define big data and describe the technologies for managing and analyzing big data.

Traditional databases rely on neatly organized content into rows and columns. Much of the data collected nowadays by companies don’t fit into that mold.

Big data describes data sets with volumes so huge they are beyond the ability of typical database management systems to capture, store, and analyze. The term doesn’t refer to any specific quantity of data but it’s usually measured in the petabyte and exabyte range. It includes structured and unstructured data captured from web traffic, email messages, and social media content like tweets and status messages. It also includes machine-generated data from sensors.

Big data contains more patterns and interesting anomalies than smaller data sets. That creates the potential to determine new insights into customer behavior, weather patterns, financial market activity, and other phenomena.

**Hadoop:** Open-source software framework that enables distributed parallel processing of huge amounts of data across inexpensive computers. The software breaks huge problems into smaller ones, processes each one on a distributed network of smaller computers, and then combines the results into a smaller data set that is easier to analyze. It uses non-relational database processing and structured, semi-structured, and unstructured data.

**In-memory computing:** Rather than using disk-based database software platforms, this technology relies primarily on a computer’s main memory for data storage. It eliminates bottlenecks that result from retrieving and reading data in a traditional database and shortens query response times. Advances in contemporary computer hardware technology makes in-memory processing possible.

**Analytic platforms:** These use both relational and non-relational technology that’s optimized for analyzing large data sets. They feature preconfigured hardware-software system designed for query processing and analytics.

List and describe the components of a contemporary business intelligence infrastructure.

Business intelligence (BI) infrastructures include an array of tools for obtaining useful information from all the different types of data used by businesses today, including semi-structured and unstructured big data in vast quantities. Data warehouses, data marts, Hadoop, in-memory processing, and analytical platforms are all included in BI infrastructures.

Powerful tools are available to analyze and access information that has been captured and organized in data warehouses and data marts. These tools enable users to analyze the data to see new patterns, relationships, and insights that are useful for guiding decision making. These tools for consolidating, analyzing, and providing access to vast amounts of data to help users make better business decisions are often referred to as business intelligence. Principal tools for business intelligence include software for database query and reporting tools for multidimensional data analysis and data mining.

Describe the capabilities of online analytical processing (OLAP).

Data warehouses support multidimensional data analysis, also known as online analytical processing (OLAP), which enables users to view the same data in different ways using multiple dimensions. Each aspect of information represents a different dimension.

OLAP represents relationships among data as a multidimensional structure, which can be visualized as cubes of data and cubes within cubes of data, enabling more sophisticated data analysis. OLAP enables users to obtain online answers to ad hoc questions in a fairly rapid amount of time, even when the data are stored in very large databases. Online analytical processing and data mining enable the manipulation and analysis of large volumes of data from many perspectives – for example, sales by item, by department, by store, or by region – in order to find patterns in the data. Such patterns are difficult to find with normal database methods, which is why a data warehouse and data mining are usually parts of OLAP.

**Define data mining, describe what types of information can be obtained from it, and explain how it differs from OLAP.**

Data mining provides insights into corporate data that cannot be obtained with OLAP by finding hidden patterns and relationships in large databases and inferring rules from them to predict future behavior. The patterns and rules are used to guide decision making and forecast the effect of those decisions. The types of information obtained from data mining include associations, sequences, classifications, clusters, and forecasts.

**Explain how text mining and web mining differ from conventional data mining.**

Conventional data mining focuses on data that have been structured in databases and files. Text mining concentrates on finding patterns and trends in unstructured data contained in text files. The data may be in emails, memos, call center transcripts, survey responses, legal cases, patent descriptions, and service reports. Text mining tools extract key elements from large unstructured data sets, discover patterns and relationships, and summarize the information.

Web mining helps businesses understand customer behavior, evaluate the effectiveness of a particular website, or quantify the success of a marketing campaign. Web mining looks for patterns in data through:

* **Web content mining:** Extracting knowledge from the content of webpages.
* **Web structure mining:** Examining data related to the structure of a particular website.
* **Web usage mining:** Examining user interaction data recorded by a web server whenever requests for a website’s resources are received.

**Explain how users can access information from a company’s internal databases through the web.**

Conventional databases can be linked via middleware to the web or a web interface to facilitate user access to an organization’s internal data. Web browser software on a client PC is used to access a corporate website over the internet. The web browser software requests data from the organization’s database, using HTML commands to communicate with the web server. Because many back-end databases cannot interpret commands written in HTML, the web server passes these requests for data to special middleware software that then translates HTML commands into SQL so that they can be processed by the DBMS working with the database. The DBMS receives the SQL requests and provides the required data. The middleware transfers information from the organization’s internal database back to the web server for delivery in the form of a webpage to the user. The software working between the web server and the DBMS can be an application server, a custom program, or a series of software scripts.

6-4 Why are information policy, data administration, and data quality assurance essential for managing the firm’s data resources?

**Define information policy and data administration and explain how they help organizations manage their data.**

An information policy specifies the organization’s rules for sharing, disseminating, acquiring, standardizing, classifying, and inventorying information. Information policy lays out specific procedures and accountabilities, identifying which users and organizational units can share information, where information can be distributed, and who is responsible for updating and maintaining the information.

Data administration is responsible for the specific policies and procedures through which data can be managed as an organizational resource. These responsibilities include developing information policy, planning for data, overseeing logical database design and data dictionary development, and monitoring how information systems specialists and end-user groups use data.

In large corporations, a formal data administration function is responsible for information policy, as well as for data planning, data dictionary development, and monitoring data usage in the firm.

**List and describe the most common data quality problems.**

Data that are inaccurate, incomplete, or inconsistent create serious operational and financial problems for businesses because they may create inaccuracies in product pricing, customer accounts, and inventory data, and lead to inaccurate decisions about what actions an organization should take. Firms must take special steps to make sure they have a high level of data quality. These include using enterprise-wide data standards, databases designed to minimize inconsistent and redundant data, data quality audits, and data cleansing software.

**List and describe the most important tools and techniques for assuring data quality.**

A data quality audit is a structured survey of the accuracy and level of completeness of the data in an information system. Data quality audits can be performed by surveying entire data files, surveying samples from data files, or surveying end users for their perceptions of data quality.

Data cleansing consists of activities for detecting and correcting data in a database that are incorrect, incomplete, improperly formatted, or redundant. Data cleansing not only corrects data but also enforces consistency among different sets of data that originated in separate information systems.

**Ch7: Review Questions**

**7-1 What are the principal components of telecommunications networks and key networking technologies?**

**Describe the features of a simple network and the network infrastructure for a large company.**

A simple network consists of two or more connected computers. Basic network components include computers, network interfaces, a connection medium, network operating system software, and either a hub or a switch. The networking infrastructure for a large company relies on both public and private infrastructures to support the movement of information across diverse technological platforms. It includes the traditional telephone system, mobile cellular communication, wireless local-area networks, videoconferencing systems, a corporate website, intranets, extranets, and an array of local and wide-area networks, including the internet. This collection of networks evolved from two fundamentally different types of networks: telephone networks and computer networks.

**Name and describe the principal technologies and trends that have shaped contemporary telecommunications systems.**

Client/server computing, the use of packet switching, and the development of widely used communications standards such as TCP/IP are the three technologies that have shaped contemporary telecommunications systems.

Client/server computing has extended to networking departments, workgroups, factory floors, and other parts of the business that could not be served by a centralized architecture. The internet is based on client/server computing. Packet switching technology allows nearly full use of almost all available lines and capacity. This was not possible with the traditional dedicated circuit-switching techniques that were used in the past. TCP/IP is a suite of protocols that has become the dominant standard of network communications. Having a set of protocols for connecting diverse hardware and software components has provided a universally agreed upon method for data transmission.

**7-2 What are the different types of networks?**

**Define an analog and a digital signal.**

**Analog:** a continuous waveform that passes through a communications medium and has been used for voice communication. Traditionally used by telephone handsets, computer speakers, or earphones.

**Digital:** a discrete, binary waveform, rather than a continuous waveform, represented by strings of two states: one bit and zero bits, which are represented as on-off electrical pulses. Computers use digital signals and require a modem to convert these digital signals into analog signals that are transmitted across telephone lines, cable lines, or wireless media.

**Distinguish between a LAN, MAN, and WAN.**

**LAN (Local Area Network):** a telecommunications network that is designed to connect personal computers and other digital devices within a half-mile or 500-meter radius. LANs typically connect a few computers in a small office, all the computers in one building, or all the computers in several buildings in close proximity. LANs require their own dedicated channels.

**MAN (Metropolitan Area Network):** a network that spans a metropolitan area, usually a city and its major suburbs. Its geographic scope falls between a WAN and a LAN.

**WAN (Wide Area Network):** spans broad geographical distances – entire regions, states, continents, or the entire globe. The most universal and powerful WAN is the internet. Computers connect to a WAN through public networks, such as the telephone system or private cable systems, or through leased lines or satellites.

7-3 How do the internet and internet technology work and how do they support communication and e-business?

**Define the internet, describe how it works, and explain how it provides business value.**

The internet is a vast network of computers that connects millions of people all over the world. The internet uses the client/server model of computing and the TCP/IP network reference model. Every computer on the internet is assigned a unique numeric IP address. No one owns the internet, and it has no formal management organization. However, worldwide internet policies are established by organizations and government bodies, such as the Internet Architecture Board and the World Wide Web Consortium. The internet must also conform to the laws of the sovereign nation-states in which it operates, as well as the technical infrastructure that exists within the nation-state.

The internet enables employees to gain remote access to the company’s internal systems through its website. They are able to better service customers and suppliers, improve operational efficiency, increase productivity, lower operational costs, have a broader market base, and reach more individual customers on a global scale by establishing a web presence. The cost of email and other internet services tend to be far lower than equivalent voice, postal, or over night delivery costs, making the internet a very inexpensive communication medium. It is also a very fast method of communication, with messages arriving anywhere in the world in a matter of seconds or minutes.

**Explain how the Domain Name System (DNS) and IP addressing system work.**

The internet is based on the TCP/IP networking protocol suite. Every computer on the internet is assigned a unique Internet Protocol (IP) address, which currently is a 32-bit number represented by four strings of numbers ranging from 0 to 255, separated by periods.

A domain name is the English-like name that corresponds to the unique 32-bit numeric IP address for each computer connected to the internet. The Domain Name System (DNS) converts IP addresses to domain names so that users only need to specify a domain name to access a computer on the internet, instead of typing the numeric IP address. DNS servers maintain a database containing IP addresses mapped to their corresponding domain names.

When a user sends a message to another user on the internet, the message is first decomposed into packets using the TCP protocol. Each packet contains its destination address. The packets are then sent from the client to the network server and from there on to as many other servers as necessary to arrive at a specific computer with a known address. At the destination address, the packets are reassembled into the original message.

**List and describe the principal internet services.**

Table 7-2 lists and describes the major internet services:

* *Email—*person-to-person messaging; document sharing.
* *Newsgroups*—discussion groups on electronic bulletin boards.
* *Chatting and instant messaging*—interactive conversations.
* *Telnet—*logging on to one computer system and doing work on another.
* *File Transfer Protocol (FTP)*—transferring files from computer to computer.
* *World Wide Web*—retrieving, formatting, and displaying information (including text, audio, graphics, and video) using hypertext links.

**Define and describe VoIP and virtual private networks and explain how they provide value to businesses.**

* *Voice over Internet Protocol (VoIP)* enables internet technology to be used for telephone voice transmission over the internet or private networks. VoIP offers the advantage of avoiding tolls charged by local and long-distance telephone networks. VoIP provides businesses an opportunity to reduce costs because they no longer have to maintain separate networks or provide support services and personnel for each different type of network. It gives organizations flexibility because phones can be added or moved to different offices without rewiring or reconfiguring networks.
* *Virtual private networks* (VPN) are secure, encrypted, private networks that have been configured within a public network to take advantage of the economies of scale and management facilities of large networks, such as the internet. VPNs are low-cost alternatives to private WANs. VPNs give businesses a more efficient network infrastructure for combining voice and data networks.

**List and describe alternative ways of locating information on the web.**

* *Search engines* are facilities on the web that help you find sites with the information and/or services you want. Examples: Google, Yahoo!, and MSN.
* *Intelligent agent shopping bots* use intelligent agent software for searching the internet for shopping information. Examples: MySimon and Froogle.
* *Blogs* are informal yet structured websites where subscribing individuals can publish stories, opinions, and links to other websites of interest.
* *Rich Site Summary or Really Simple Syndication (RSS)* is a simple way for people to have content they want pulled from websites and fed automatically to their computers, where it can be stored for later viewing. It’s commonly used with blogs.
* *Wikis* are collaborative websites where visitors can add, delete, or modify content on the site, including the work of previous authors.
* *Web 2.0* provides second-generation interactive internet-based services that enable people to collaborate, share information, and create new services online. Web 2.0 software applications run on the web itself, instead of the desktop, and bring the vision of web-based computing closer to realization.
* *Web 3.0 (Semantic Web)* reduces the amount of human involvement in searching for and processing web information. It’s still in its infancy but promises to establish specific meanings for data on the web, categories for classifying the data, and relationships between classification categories.

**Describe how online search technologies are used for marketing.**

Search engine marketing monetizes the value of the search process. Searching is one of the web’s most popular activities with billions of queries performed each month. Search engines are the foundation for the most lucrative form of online marketing and advertising. When users enter a search term in a search engine, they receive two types of listings: sponsored links, for which advertisers have paid to be listed, and unsponsored organic search results. Advertisers can also purchase small text boxes on the side of search results pages. Paid, sponsored advertisements are the fastest growing form of internet advertising and are powerful new marketing tools that precisely match consumer interests with advertising messages at the right moment.

7-4 What are the principal technologies and standards for wireless networking, communications, and internet access?

**Define Bluetooth, Wi-Fi, WiMax, and 3G and 4G networks.**

Standards for wireless computer networks include Bluetooth (802.15) for small personal-area networks (PANs), Wi-Fi (802.11) for local-area networks (LANs), and WiMax (802.16) for metropolitan-area networks (MANs). Bluetooth can link up to eight devices within a 10-meter area using low-power, radio-based communication, and can transmit up to 722 Kbps in the 2.4 GHz band. Wireless phones, keyboards, computers, printers, and PDAs using Bluetooth can communicate with each other and even operate each other without direct user intervention.

Wi-Fi is useful for creating wireless LANs and for providing wireless internet access. Its access range is limited to anywhere between 300 feet and three miles. Hotspots are public access points individuals use to obtain high speed internet access.

WiMax has a wireless access range of up to 31 miles and a data transfer rate of up to 75 Mbps, making it suitable for providing broadband internet access in areas lacking DSL and cable lines. The 802.16 specification also has robust security and quality-of-service features to support voice and video.

*3G* is a short term for third-generation wireless technology, especially mobile communications. Cellular networks have evolved from slow-speed (1G) analog networks to high-speed, high-bandwidth, digital packet-switched, third-generation (3G) networks with speeds ranging from 144 Kbps to more than 2 Mbps for data transmission.

*4G* is a short term for fourth-generation wireless technology. It is entirely packet-switched and capable of 100 Mbps transmission speed (which can reach 1 Gbps under optimal conditions), with premium quality and high security. Voice, data, and high-quality streaming video are available to users anywhere, anytime.

Describe the capabilities of each principal technology and for which types of applications each is best suited.

* + Bluetooth: Access very limited; useful for creating small personal-area networks.
  + Wi-Fi: Access is limited to 30–50 meters; useful for creating small local area networks.
  + WiMax: Access is limited to a range up to 31 miles: useful for creating wide area networks.
  + 3G networks: Access is available on major cellular telephone carriers that have configured their networks for 3G services.
  + 4G networks: Provides premium quality for voice, data, and streaming video from cellular telephone carriers.

Define RFID, explain how it works, and describe how it provides value to businesses.

Mobile wireless technology facilitates supply chain management by capturing data on the movement of goods in real-time and by providing detailed, immediate information as goods move among supply chain partners. Radio frequency identification (RFID) systems provide a microchip that contains data about an item and its location. The tags transmit radio signals over a short distance to special RFID readers. The RFID readers then pass the data over a network to a computer for processing.

RFID gives businesses an opportunity to further automate their supply chain networks. The technology allows more data on an RFID chip than typical barcodes. RFID systems track each pallet, lot, or unit item in a shipment. The technology helps companies improve receiving and storage operations by improving their ability to “see” exactly what stock is stored in warehouses or on retail store shelves.

Define WSNs, explain how they work, and describe the kinds of applications that use them.

Wireless sensor networks (WSNs) are networks of interconnected wireless devices with some processing and radio-transmitting capability that are embedded into the physical environment to provide measurements of many points over large spaces.

Wireless sensor networks are valuable for monitoring environmental changes, traffic patterns, security incidents, or supply chain events. Wireless sensor networks can be placed in the field for years without any maintenance or human intervention. That reduces costs to businesses using them.

**Ch8: Review Questions**

**8-1 Why are information systems vulnerable to destruction, error, and abuse?**

**List and describe the most common threats against contemporary information systems.**

The most common threats against contemporary information systems include: technical, organizational, and environmental factors compounded by poor management decisions. Figure 8-1 includes the following:

* Technical: Unauthorized access, introducing errors.
* Communications: Tapping, sniffing, message alternation, theft and fraud, radiation.
* Corporate servers: Hacking, viruses and worms, theft and fraud, vandalism, denial of service attacks.
* Corporate systems: Theft of data, copying data, alteration of data, hardware failure, and software failure. Power failures, floods, fires, or other natural disasters can also disrupt computer systems.
* Poor management decisions: Poorly designed safeguards that protect valuable data from being lost, destroyed, or falling into the wrong hands.

**Define malware and distinguish among a virus, a worm, and a Trojan horse.**

Malware (for malicious software) is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware programs that gather information about a computer user without permission.

* *Virus:* A program or programming code that replicates itself by being copied or initiating its copying to another program, computer boot sector, or document.
* *Worm:* A self-replicating virus that does not alter files but resides in active memory and duplicates itself without human intervention.
* *Trojan horse:* A program in which malicious or harmful code is contained inside apparently harmless programming or data. A Trojan horse is not itself a virus because it does not replicate but is often a way for viruses or other malicious code to be introduced into a computer system.

**Define hacker and explain how hackers create security problems and damage systems.**

A hacker is an individual who gains unauthorized access to a computer system by finding weaknesses in security protections used by websites and computer systems. Hackers not only threaten the security of computer systems, but they also steal goods and information, damage systems, and commit cybervandalism. They may intentionally disrupt, deface, or even destroy a website or corporate information system.

**Define computer crime. Provide two examples of crime in which computers are targets and two examples in which computers are used as instruments of crime.**

The Department of Justice defines computer crime as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution.” Computer crime is defined as the commission of illegal acts through the use of a computer or against a computer system. Table 8-2 provides examples of computer crimes.

Computers as targets of crime:

* Breaching the confidentiality of protected computerized data.
* Accessing a computer system without authority.
* Knowingly accessing a protected computer to commit fraud.
* Intentionally accessing a protected computer and causing damage, negligently or deliberately.
* Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer.
* Threatening to cause damage to a protected computer.

Computers as instruments of crime:

* Theft of trade secrets.
* Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and videos.
* Schemes to defraud.
* Using email for threats or harassment.
* Internationally attempting to intercept electronic communication.
* Illegally accessing stored electronic communications, including email and voice mail.
* Transmitting or processing child pornography using a computer.

**Define identity theft and phishing and explain why identity theft is such a big problem today.**

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as social security identification number, driver’s license number, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials.

It is a big problem today as the internet has made it easy for identity thieves to use stolen information because goods can be purchased online without any personal interaction. Credit card files are a major target of website hackers. Moreover, e-commerce sites are wonderful sources of customer personal information that criminals can use to establish a new identity and credit for their own purposes.

Phishing involves setting up fake websites or sending email messages that look like those of legitimate businesses to ask users for confidential personal data. The email instructs recipients to update or confirm records by providing social security numbers, bank and credit card information, and other confidential data either by responding to the email message or by entering the information at a bogus website. New phishing techniques such as evil twins and pharming are very hard to detect.

**Describe the security and system reliability problems employees create.**

The largest financial threats to business institutions come from employees. Some of the largest disruptions to service, destruction of e-commerce sites, and diversion of customer credit data and personal information have come from insiders. Employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization’s systems without leaving a trace.

Many employees forget their passwords to access computer systems or allow other coworkers to use them, which compromises the system. Malicious intruders seeking system access sometimes trick employees into revealing their passwords by pretending to be legitimate members of the company in need of information (social engineering). Employees can introduce errors by entering faulty data or by not following proper instructions for processing data and using computer equipment. Information specialists can also create software errors as they design and develop new software or maintain existing programs.

**Explain how software defects affect system reliability and security.**

Software can fail to perform, perform erratically, or give erroneous results because of undetected bugs. A control system that fails to perform can lead to medical equipment that fails or telephones that do not carry messages or allow access to the internet. A business system failing could mean customers are under- or over-billed. Or, it could mean that the business orders more inventory than it needs. Or an automobile’s braking system may fail.

Major quality problems are the bugs or defects caused by incorrect design. The other problem is maintenance of old programs caused by organizational changes, system design flaws, and software complexity. Bugs in even mildly complex programs can be impossible to find in testing, making them hidden bombs.

**8-2 What is the business value of security and control?**

**Explain how security and control provide value for businesses.**

Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.

Controls consist of all the methods, policies, and organizational procedures that ensure the safety of the organization’s assets; the accuracy and reliability of its account records; and operational adherence to management standards.

The business value of security and control:

* Firms relying on computer systems for their core business functions can lose sales and productivity.
* Information assets, such as confidential employee records, trade secrets, or business plans, lose much of their value if they are revealed to outsiders or if they expose the firm to legal liability.

**Describe the relationship between security and control and recent U.S. government regulatory requirements and computer forensics.**

Legal actions requiring electronic evidence and computer forensics also require firms to pay more attention to security and electronic records management. Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law. It deals with the following problems:

* Recovering data from computers while preserving evidential integrity.
* Securely storing and handling recovered electronic data.
* Finding significant information in a large volume of electronic data.
* Presenting the information to a court of law.

Recent U.S. government regulatory requirements include:

* Health Insurance Portability and Accountability Act (HIPAA)
* Gramm-Leach-Bliley Act
* Sarbanes-Oxley Act

These laws require companies to practice stringent electronic records management and adhere to strict standards for security, privacy, and control.

**8-3 What are the components of an organizational framework for security and control?**

**Define general controls and describe each type of general control.**

General controls govern the design, security, and use of computer programs and the security of data files in general throughout the organization’s information technology infrastructure. They apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over implementation of system processes, and administrative controls. Table 8-3 describes each type of general control.

**Define application controls and describe each type of application control.**

Application controls are specific controls unique to each computerized application. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application.

Application controls can be classified as:

* **Input controls:** Check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling.
* **Processing controls:** Establish that data are complete and accurate during updating.
* **Output controls:** Ensure that the results of computer processing are accurate, complete, and properly distributed.

**Describe the function of risk assessment and explain how it is conducted for information systems.**

A risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled. Business managers working with information systems specialists can determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage. Controls can be adjusted or added to focus on the areas of greatest risk. An organization does not want to over-control areas where risk is low or under-control areas where risk is high.

Security risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all of the firm’s risks, and ranking those risks by level of severity. This process involves making cost-effective decisions on what you want to protect. The old security adage says that you should not spend more to protect something than it is actually worth. Two elements of a risk analysis that should be considered are: (1) identifying the assets and (2) identifying the threats. For each asset, the basic goals of security are availability, confidentiality, and integrity. Each threat should be examined with an eye on how the threat could affect these areas. One step in a risk analysis is to identify all the things that need to be protected. Some things are obvious, like all the various pieces of hardware, but some are overlooked, such as the people who actually use the systems. The essential point is to list all things that could be affected by a security problem.

**Define and describe the following: security policy, acceptable use policy, and identity management.**

A security policy consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals. The security policy drives policies determining acceptable use of the firm’s information resources and which members of the company have access to its information assets.

An acceptable use policy (AUP) defines acceptable uses of the firm’s information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the internet. The policy should clarify company policy regarding privacy, user responsibility, and personal use of company equipment and networks. A good AUP defines unacceptable and acceptable actions for each user and specifies consequences for noncompliance.

Identity management consists of business processes and software tools for identifying valid system users and controlling their access to system resources. It includes policies for identifying and authorizing different categories of system users, specifying what systems or portions of systems each user is allowed to access, and the processes and technologies for authenticating users and protecting their identities.

**Explain how information systems auditing promotes security and control.**

Comprehensive and systematic MIS auditing organizations determine the effectiveness of security and controls for their information systems. An MIS audit identifies all of the controls that govern individual information systems and assesses their effectiveness. Control weaknesses and their probability of occurrence will be noted. The results of the audit can be used as guidelines for strengthening controls, if required.

**8-4 What are the most important tools and technologies for safeguarding information resources?**

**Name and describe three authentication methods.**

Authentication refers to the ability to know that a person is who he or she claims to be. Some methods are described below:

* What you know: Passwords known only to the authorized users.
* What you have:
  + A token is a physical device that is designed to provide the identity of a single user.
  + A smart card is a device that contains a chip formatted with access permission and other data.
* What you are: Biometrics is based on the measurement of a physical or behavioral trait that makes each individual unique.

**Describe the roles of firewalls, intrusion detection systems, and antivirus software in promoting security.**

A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. Firewalls prevent unauthorized users from accessing internal networks. They protect internal systems by monitoring packets for the wrong source or destination; by offering a proxy server with no access to the internal documents and systems; or by restricting the types of messages that get through (for example, email). Further, many authentication controls have been added for webpages as part of firewalls.

Intrusion detection systems monitor the most vulnerable points or “hot spots” in a network to detect and deter unauthorized intruders. These systems often also monitor events as they happen to look for security attacks in progress. Sometimes they can be programmed to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

Antivirus software is designed to check computer systems and drives for the presence of computer viruses and worms and often eliminates the malicious software, whereas antispyware software combats intrusive and harmful spyware programs. Often the software can eliminate the virus from the infected area. To be effective, antivirus software must be continually updated.

**Explain how encryption protects information.**

Encryption, the coding and scrambling of messages, is a widely used technology for securing electronic transmissions over the internet and over Wi-Fi networks. Encryption offers protection by keeping messages or packets hidden from the view of unauthorized readers. Encryption is crucial for ensuring the success of electronic commerce between the organization and its customers, and between the organization and its vendors.

**Describe the role of encryption and digital certificates in a public key infrastructure.**

Digital certificates combined with public key encryption provide further protection of electronic transactions by authenticating a user’s identity. Digital certificates are data fields used to establish the identity of the sender and to provide the receiver with the means to encode a reply. They use a trusted third party known as a certificate authority to validate a user’s identity. Both digital signatures and digital certificates play a role in authentication. Authentication refers to the ability of each party to know that the other parties are who they claim to be.

**Distinguish between disaster recovery planning and business continuity planning.**

Disaster recovery planning devises plans for the restoration of computing and communications services after they have been disrupted by an event such as an earthquake, flood, or terrorist attack. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.

Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down.

**Identify and describe the security problems cloud computing poses.**

Accountability and responsibility for protection of sensitive data reside with the company owning that data, even though it’s stored offsite. The company needs to make sure its data are protected at a level that meets corporate requirements. The company should stipulate to the cloud provider how its data are stored and processed in specific jurisdictions according to the privacy rules of those jurisdictions. The company needs to verify with the cloud provider how its corporate data are segregated from data belonging to other companies and ask for proof that encryption mechanisms are sound. The company needs to verify how the cloud provider will respond if a disaster strikes. Will the cloud provider be able to completely restore the company’s data and how long will that take? Will the cloud provider submit to external audits and security certifications?

**Describe measures for improving software quality and reliability.**

Using software metrics and rigorous software testing are two measures for improving software quality and reliability.

Software metrics are objective assessments of the system in the form of quantified measurements. Metrics allow an information systems department and end users to jointly measure the performance of a system and identify problems as they occur. Metrics must be carefully designed, formal, objective, and used consistently. Examples of software metrics include:

* Number of transactions that can be processed in a specified unit of time.
* Online response time.
* Number of known bugs per hundred lines of program code.

Early, regular, and thorough testing will contribute significantly to system quality. Testing can prove the correctness of work but also uncover errors that always exist in software. Testing can be accomplished through the use of:

* Walkthroughs: A review of a specification or design document by a small group of people.
* Coding walkthroughs: Once developers start writing software, these can be used to review program code.
* Debugging: When errors are discovered, the source is found and eliminated.